CLAIMS

1. A cryptographic method that can be used in a transaction for which a first entity (A) generates, by means of an RSA private key (d), a proof verifiable by a second entity (B) by means of an RSA public key associated with said private key, said public key comprising a first exponent (e) and a modulus (n), characterized in that:

- the first entity (A) generates a first element of proof (x), a first calculation of which, consuming considerable resources, can be executed independently of the transaction;
- the first entity (A) generates a second element of proof (y) related to the first element of proof (x) and dependent on a common number (c) shared by the first and second entities specifically for the transaction, a second calculation of which consumes few resources; and
- the second entity (B) verifies that the first element of proof (x) is related through a relationship with a first power modulo the modulus (n) of a generic number (g) having a second exponent equal to a linear combination of all or part of the common number (c) and of the first exponent (e) of the public key multiplied by the second element of proof (y).

2. The cryptographic method as claimed in claim 1, characterized in that, to allow the first entity (A) to be identified:

- the first element of proof (x) is generated by the first entity (A) by raising the generic number (g) to a second power modulo the modulus (n) having a third exponent equal to the first exponent (e) of the public key multiplied by a random integer (r) kept secret by the first entity (A);
- the common number (c) is chosen randomly from

within a security interval [0,t-1] and then sent by the second entity (B) after having received the first element of proof (x); and

- the relationship verified by the second entity (B) is an equality relationship between a power of the first element of proof (x) and the first power of the generic number (g).

3. The cryptographic method as claimed in claim 1, characterized in that, in order to allow a message (M) to be signed:

- the first element of proof (x) is generated by the first entity (A) by applying a standard hash function to the message (M) and to the generic number (g) raised to a second power modulo the modulus (n) having a third exponent equal to the first exponent (e) of the public key multiplied by a random integer (r) kept secret by the first entity (A);

- the common number (c) is equal to the first element of proof (x); and

- the relationship verified by the second entity (B) is an equality relationship between the first element of proof (x) and a result of the standard hash function applied to the message (M) and to the first power of the generic number (g).

4. The cryptographic method as claimed in claim 1, characterized in that, in order to authenticate that a message (M) received by the second entity (B) comes from the first entity (A):

- the first element of proof (x) is generated by the first entity (A) by applying a standard hash function to the message (M) and to the generic number (g) raised to a second power modulo the modulus (n) having a third exponent equal to the first exponent (e) of the public key multiplied by a random integer (r) kept secret by the first entity (A);

- the common number (c) is chosen at random from within a security interval [0,t-1] and then sent by the

second entity (B) after having received the first element of proof (x); and

- the relationship verified by the second entity (B) is an equality relationship between the first element of proof (x) and a result of the standard hash function applied to the message (M) and to the first power of the generic number (g).

5. The cryptographic method as claimed in one of claims 2 to 4, characterized in that:

- the second element of proof (y) is generated by the first entity (A) by subtracting, from the random integer (r), the private key (d) multiplied by the common number (c);

- the linear combination equal to the second exponent comprises a positive unitary coefficient for the common number (c) and a positive unitary coefficient for the first exponent (e) of the public key multiplied by the second element of proof (y); and

- in the verified relationship, the first element of proof is considered with a unitary exponent power.

6. The cryptographic method as claimed in either of claims 2 and 4, characterized in that:

- since the common number (c) is split into a first elementary common number (a) and a second elementary common number (b), the second element of proof (y) is generated by the first entity (A) by subtracting, from the random integer (r) multiplied by the first elementary common number (a), the private key (d) multiplied by the second elementary common number (b);

- the linear combination equal to the second exponent comprises a zero coefficient for the first elementary common number (a), a positive unitary coefficient for the second elementary common number (b) and a positive unitary coefficient for the first exponent (e) of the public key multiplied by the second element of proof (y); and

- in the verified relationship, the first element of proof is considered with an exponent power equal to the first elementary common number (a).

7. The cryptographic method as claimed in either of claims 5 and 6, characterized in that the second element of proof (y) is calculated modulo an image of the modulus (n) via a Carmichael function (λ) or modulo a multiple of the order of the generic number (g) modulo the modulus (n).

8. The cryptographic method as claimed in either of claims 5 and 6, characterized in that the random number (r) is very much greater than the value of the private key (d).

9. The cryptographic method as claimed in claim 7, characterized in that the random integer (r) is less than an image of the modulus (n) via a Carmichael function (λ) or less than a multiple of the order of the generic number (g) modulo the modulus (n).

10. The cryptographic method as claimed in one of claims 5 to 9, characterized in that the third exponent is calculated modulo an image of the modulus (n) via a Carmichael function (λ) or modulo a multiple of the order of the generic number (g) modulo the modulus (n).

11. The cryptographic method as claimed in one of the preceding claims, characterized in that the generic number (g) is transmitted with the public key, the generic number (g) being equal to a simple number (G) raised to a power modulo the modulus (n) with the private key (d) as exponent.

12. The cryptographic method as claimed in one of the preceding claims, characterized in that:

- a third entity (C) receives the second element of proof (y), generates a third element of proof (Y) by

raising the generic number (g) to a power modulo the modulus (n) with the second element of proof (y) as exponent and sends the third element of proof (Y) to the second entity (B); and

- the second entity (B), modulo the modulus (n), raises the third element of proof (Y) to a power of first exponent (e) and multiplies the result thereof by the generic number (g) raised to a power whose exponent is the common number (c) in order to verify the relationship relating the first element of proof to the second element of proof.

13. A prover device (30) provided with an RSA private key (d) kept secret and protected against intrusions, for generating, during a transaction with a verifier device, a proof whose verification by means of a public key associated with said private key makes it possible to guarantee that the device (30) has originated said proof, said RSA public key comprising a first exponent (e) and a modulus (n), characterized in that it comprises:

- calculation means (37) designed to generate a first element of proof (x) completely or partly independently of the transaction and to generate a second element of proof (y) related to the first element of proof and dependent on a common number (c) specific to the transaction; and

- communication means (34) designed to transmit at least the first and second elements of proof and designed to transmit said common number (c) to the verifier device or to receive said common number therefrom.

14. The prover device (30) as claimed in claim 13, characterized in that:

- the calculation means (37) are, on the one hand, designed to generate a first random number (r) and to raise a generic number (g) to a second power modulo the modulus (n) having a third exponent equal to

the first exponent (e) of the public key multiplied by the random integer (r); and

- the calculation means (37) are, on the other hand designed to generate the second element of proof (y) by taking the difference between the random integer (r) and the private key (d) multiplied by the common number (c) or the common number (c) being split into two elementary common numbers (a, b), by subtracting from the random integer (r) multiplied by the first elementary common number (a), the private key (d) multiplied by the second elementary common number (b).

15. The prover device (30) as claimed in claim 14, characterized in that the calculation means (37) are designed to carry out operations modulo an image of the modulus (n) via a Carmichael function (λ) or modulo a multiple of the order of the generic number (g) modulo the modulus (n).

16. A verifier device (31) for verifying that a proof originates from a prover device provided with an RSA private key (d) kept secret by the prover device, by means of a public key associated with said private key, said RSA public key comprising an exponent (e) and a modulus (n), characterized in that it comprises:

- communication means (35) designed to receive a first element of proof (x) and a second element of proof (y) or a third element of proof (Y), and to receive or transmit a common number (c) specific to a transaction within which the first and the second or the third element of proof are received; and

- calculation means (38) designed to verify that the first element of proof (x) is related through a relationship, modulo the modulus (n), with a first power of a generic number (g) having a second exponent equal to a linear combination of all or part of the common number (c) and of the first exponent (e) of the public key multiplied by the second element of proof (y).

17. The verifier device (31) as claimed in claim 16, characterized in that the communication means are designed to receive the second element of proof (y) and in that the calculation means (38) are designed to calculate the second exponent and said first power of the generic number (g).

18. The verifier device (31) as claimed in claim 16, characterized in that the communication means are designed to receive the third element of proof (Y) and in that the calculation means (38) are designed to raise the third element of proof (Y) to a power of the first exponent (e) of the public key in order to multiply the result thereof by the generic number (g) raised to a second power having the common number (c) as exponent.